高校网络安全工作必知100个知识名词（2025版）

随着数字化校园建设的加速推进，高校网络安全问题日益突出。无论是数据泄露、勒索病毒，还是钓鱼攻击、供应链安全风险，都可能对学校的教学、科研和管理造成严重影响。

作为高校网络安全工作者和有关师生，必须掌握全面的安全知识，才能有效应对各类威胁。本文整理了100个高校网络安全核心知识点，涵盖政策法规、技术防护、应急响应、数据安全、安全意识等多个方面，帮助您构建全面的安全防护体系。

一、政策法规与标准（1-15）

1.《网络安全法》：高校必须落实网络安全等级保护制度（等保2.0）。

2.《数据安全法》：明确数据分类分级要求，防止数据泄露和滥用。

3.《个人信息保护法》：保护师生个人信息，禁止非法收集、使用和泄露。

4.《密码法》：高校应采用商用密码保护敏感数据。

5.《反电信网络诈骗法》：防范钓鱼邮件、诈骗电话等针对师生的攻击。

6.《关键信息基础设施安全保护条例》：参照关基条例，高校核心系统（如教务、财务）需重点防护。

7.《网络安全审查办法》：采购 IT 产品需进行安全审查，防止供应链风险。

8.《信息安全技术网络安全等级保护基本要求（GB/T22239-2019）》：高校信息系统需定级备案，三级系统每年测评，二级系统每两年测评。

9.《教育行业信息系统安全等级保护定级工作指南（试行）》：教育部对信息系统安全等级保护定级工作的专项要求。

10.《网络安全漏洞管理规定》：高校发现漏洞需及时修复并上报。

11.《国家网络安全事件应急预案》：高校需结合校园实际，制定本校应急预案。

12.《教育系统网络安全事件应急预案》：明确网络安全事件分级及处置流程。

13.《网络数据安全管理条例》：高校需规范数据全生命周期管理。

14.《数据出境安全评估办法》：涉及国际合作的科研数据需合规出境。

15.《教育行业数据分类分级指南》：数据分级和分类，明确哪些数据属于敏感数据。

二、网络安全技术（16-45）

（一）边界防护技术

16.防火墙（FW）：校园网边界防护的第一道防线（分为出口、数据中心防火墙）。

17.Web 应用防火墙（WAF）：保护网站（Web 应用）免受 SQL 注入、XSS 攻击。

18.VPN 安全：通过公共网络远程访问校园内网资源时，通过加密技术建立安全连接。

19.DNS 安全：防止 DNS 劫持，采用 DNSSEC。禁止访问不安全的域名。

20.Wi-Fi 安全:校园无线网需采用 WPA3 加密,禁用 WEP。

21.网络分段：将一个大的网络划分成多个小的网络段，以提高安全性和管理效率。避免某一区域被攻破后扩散至核心系统。

22.身份和访问管理（IAM）：一种管理和控制用户身份及其权限的技术框架。

23.多因素认证：一种身份验证方法，要求用户提供两个或更多的证明身份的因素，如密码、指纹扫描、硬件令牌等。

（二）终端与服务器防护

24.终端安全防护（EDR）：防止勒索病毒、木马感染。

25.物联网安全：监控摄像头、智能设备需安全配置。

26.服务器加固:关闭非必要端口,禁用“root”“admin”等默认账号，每月定期更新系统及应用软件补丁。

27.堡垒机：运维人员必须通过堡垒机访问服务器。

28.零信任架构（ZTA）：假设网络环境中的任何用户或设备都是不可信的。取代传统 VPN，实现动态访问控制。

（三）监测与响应技术

29.入侵检测/防御系统（IDS/IPS）：实时监测网络攻击行为。主动拦截恶意流量。

30.漏洞扫描：定期扫描系统漏洞，及时修复高危漏洞。

31.渗透测试：模拟黑客攻击的方法，用于评估系统、网络或应用程序的安全性。

32.网络流量分析（NTA）：监控和分析网络流量，用于检测异常模式和潜在的安全威胁。识别恶意活动和漏洞利用。

33.态势感知平台：实时监控全网安全态势。

34.威胁情报（TI）：这些情报可以帮助组织预防和应对网络攻击。需要订阅安全厂商威胁情报，提前预警。

35.暗网监测：监测学校数据是否在暗网被售卖。

36.邮件安全：防范钓鱼邮件，部署SPF/DKIM/DMARC。

37.日志审计：全校系统日志（网络设备、服务器、终端）需集中存储，留存6个月以上，便于溯源分析。

38.APT防护：防范高级持续性威胁（如国家级黑客攻击）。

39.蜜罐技术：诱捕攻击者，分析攻击手法。

（四）数据与备份技术

40.数据加密：敏感数据存储和传输需加密（如AES、RSA）。

41.数据脱敏：公开数据需脱敏处理，防止隐私泄露。

42.备份与恢复：关键数据每日备份，定期演练恢复流程。

43. 数字证书：一种由证书颁发机构（CA）签发的电子文件，用于证明证书持有者的身份或公钥的有效性。

44. SSL/TLS 协议：SSL（安全套接层）和 TLS（传输层安全）协议是用于在网络上提供安全通信的协议。它们通过加密数据传输、验证服务器和客户端身份等方式，确保数据在网络中的安全性。

45. 网络安全威胁：包含外部攻击者、内部人员、系统自身脆弱性、自然灾害和意外事故。

三、数据安全（46-60）

46. 数据分类分级：区分公开数据、内部数据、敏感数据、机密数据。

47. 数据资产盘点：建立“全校数据资产清单”，明确“数据类型+存储位置+责任人+防护措施”。

48. 数据生命周期管理：从采集、存储、使用到销毁的全流程保护。

49. 数据泄露防护（DLP）：防止师生误发敏感数据。

50. 数据库加密：保护存储在数据库中的敏感数据。通过对数据进行加密，即使物理介质被盗或泄露，也无法读取其中的内容。。

51. 数据库防火墙/审计：配置数据库访问控制、审计日志。监控敏感数据访问行为。

52. 数据水印：防止内部人员泄露数据，可溯源追责。

53. 数据销毁：硬盘报废前需彻底擦除数据。

54.数据备份策略：3-2-1 原则（3 份备份，2 种介质，1 份离线）。

55.API 安全：应用程序接口（API）的安全风险，如未授权访问、注入攻击等。

56.数据合规审计：定期检查数据使用是否符合法规。

57.数据安全事件响应：发生泄露后如何快速处置？

58.数据安全培训：师生需了解数据保护基本规则。

59.数据安全风险评估：每年至少一次全面风险评估。

60.数据安全应急预案：制定数据泄露应急响应流程。

四、安全意识与培训（61-70）

61.钓鱼邮件识别：如何辨别？①查发件人邮箱②看内容细节③验链接/附件。

62.弱密码风险：禁止使用“123456”“admin”等简单密码。；每 90 天更换 1 次密码。

63.社会工程学攻击：防范假冒 IT 人员骗取账号密码。

64.U 盘安全：外来 U 盘需杀毒后再使用。

65.公共 Wi-Fi 风险：避免在咖啡厅通过不清楚的 WiFi 访问重要系统、登录校园 VPN。

66.账号权限安全：离职员工账号需及时注销。删除办公电脑敏感数据。

67.安全事件报告：发现安全事件应立即上报，不得隐瞒。

68.安全演练：每年至少一次网络安全应急演练。

69. 安全宣传周：利用“国家网络安全宣传周”（9 月）提升师生安全意识。

70. 安全培训考核：新入职教职工、新生入学、新任职信息系统管理员，需完成“网络安全培训”并通过考核。

五、应急响应（71-85）

71. 网络安全事件分级：一般、较大、重大、特别重大。

72. 应急预案：高校需制定网络安全事件应急预案。

73. 应急响应流程：发现→报告→分析→处置→恢复→总结。

74. 勒索病毒应急：立即断网，禁用共享，恢复备份。

75. DDoS 攻击应急：启用流量清洗，联系 ISP 协助。

76. 网站篡改应急：关闭网站，排查后门，恢复备份。

77. 数据泄露应急：阻断泄露途径，溯源泄露源头，通知受影响人员。

78. 漏洞利用应急：临时关闭漏洞端口，打补丁修复。

79. 恶意软件清除：使用杀毒工具全盘扫描。

80. 日志分析：通过日志追踪攻击源头。

81. 取证与溯源：保留攻击证据，必要时报警。

82. 第三方协作：联系安全厂商、公安网安协助处置。

83. 事后复盘：撰写安全事件报告，优化防护策略。

84. 灾备演练：每年至少一次数据恢复演练。

85. 红蓝对抗演练：每半年开展 1 次模拟黑客攻击，检验防御能力。

六、管理规范（86-100）

86. 安全责任制：校领导是第一责任人，信息中心主任、业务系统管理部门领导是直接责任人。系统管理员、业务管理人员为岗位责任人。；每年签订《网络安全责任书》，明确考核与追责条款。

87. 安全管理制度：制定“1+N”制度体系，包含账号管理、运维管理、数据管理、应急响应、外包管理等制度。

88. 安全审计：定期检查系统配置是否符合安全要求。

89. 外包安全管理：第三方运维需签订保密协议。提供员工背景审查材料，禁止访问核心数据，外包服务结束后，立即回收所有权限。

90. 供应链安全：管理和保护产品或服务供应链中的各个环节，以防止恶意活动或安全漏洞对供应链造成影响。

91. 资产管理：建立全校 IT 资产清单，包括 IP、系统、责任人。每季度更新 1 次清单，避免“僵尸设备”。

92. 漏洞管理：建立“漏洞全生命周期管理流程”：发现漏洞（扫描/情报）→分级（高危/中危/低危）→派发整改（责任人+时限）→验证修复→闭环归档。未按时整改的，约谈部门负责人。

93. 变更管理：系统升级、配置变更需审批并记录。禁止“未经审批的变更”。

94. 安全考核：将网络安全纳入部门/个人年度考核。

95. 安全预算：每年预留网络安全专项经费。占 IT 总预算比例不低于 15%。

96. 安全岗位设置：需配备专职安全管理员，不可兼职。安全人员需定期参加“技能培训”。

97. 安全合规检查：接受教育部、公安部的网络安全检查。对检查发现的问题，及时完成整改并提交报告。

98. 安全文化建设：通过“安全月报”、“安全专栏”、“安全表彰”，推动全校形成“网络安全人人有责”的氛围。

99. 国际标准参考：ISO27001、NISTCSF 等框架的借鉴。

100. 持续改进：每半年开展“安全体系评审”，结合“安全事件处置情况”“演练结果”“法规更新”，调整防护策略；每年发布“网络安全年度报告”。

总结

高校网络安全是一项系统性工程，涉及技术、管理、法律、意识等多个层面。作为网络安全工作者，以及校园师生，必须不断学习最新安全知识，掌握防护技能，才能有效应对日益复杂的网络威胁。